

FinTech: Shaping the Financial World

April 13, 2020

Class 5: Overview

- The Internet and the Payment Riddle
- Money
- Satoshi Nakamoto's Innovation
- Crypto Markets
- Blockchain Technology Use Cases
- Challenges & Assessing Viability of Use Cases
- Central Bank Digital Currencies
- Ground Truths

Class 5: Readings

- *'Even if a Thousand Projects Don't Make It, Blockchain Is Still a Change Catalyst'* Gensler, CoinDesk
- *'Economics of Money & Blockchain Technology and Evaluating Projects'* MIT Cryptocurrency Online Course
- *'Responses from Big Finance'* MIT Cryptocurrency Online Course
- *'The technology of retail central bank digital currency'* Bank of International Settlement

Class 5: Study Questions

- How does Bitcoin fit within the history of money, the emergence of the Internet and failed attempts of cryptographic payment systems?
- What are the strategic and tactical considerations in assessing the viability and value proposition of a blockchain technology project? How can you separate rigorous analysis from mere assertion and hype in the blockchain ecosystem?
- What strategic considerations should go into Central Banks thinking of expanding access to digital reserves through central bank digital currency (CBDC)?



'The Net' opening scene

1995

Sandra Bullock

Internet and the Payments Riddle

- How to Move Value on the Internet
 - Securely
 - Efficiently
 - As a Packet of Data – Peer to Peer
 - While Prohibiting Double Spending

Early Cryptographic Digital Currencies ... Failed

Notable Efforts

- DigiCash (1994), Mondex (1994), CyberCash (1994)
- E-gold (1996), Hashcash (1997)
- Bit Gold (1998), B-Money (1998), Lucre (1999)

Hurdles

- Merchant adoption
- Centralization
- Double Spending
- Consensus

Early Digital & Mobile Payment Solutions

Secure Socket Layer
Transport Layer Security

SSL / TLS - 1996

Cryptographic Protocols for
Secure Network Communication



Money

Plato:

- Money is a 'symbol' devised for the purpose of exchanges
- Opposed using gold or silver for money

Aristotle:

- Solves the 'problem of commensurability'
- 'Money is a guarantee that we may have what we want in the future. Though we need nothing at the moment it insures the possibility of satisfying a new desire when it arises.'
- Four absolutes to have 'Universal Value':
 - Durable, Portable, Divisible & Intrinsic Value

Modern Characteristics:

- Durable, Portable, Divisible, Uniform, Acceptable, & Stable



Image is in the public domain.

What is the Role of Money?



© Source Unknown. All rights reserved. This content is excluded from our Creative Commons license. For more information, see <https://ocw.mit.edu/help/faq-fair-use/>

Medium of Exchange



Image by [Rob Pongsajapan](#) on flickr. CC BY.

Store of Value



Image by [ajalfaro](#) on flickr. CC BY-NC-SA

Unit of Account

Money



Image is in the public domain.

Cowrie Shells
Nigeria



Image by [Daderot](#) on Wikimedia. License: CC0.

Silver Dekadrachm
Greece



Image is in the public domain.

Jiaozi Promissory Note
Song Dynasty China



Image is in the public domain.

Private Bank Notes
United States



Image by [epSos.de](#) on Wikimedia. CC BY

Fiat Paper Money



Image by [markus 119](#) on Flickr. CC BY

Alipay Mobile Wallet
China

Fiat Currency

- Represented by:
 - Central Bank Notes
 - Central Bank Reserves &
 - Commercial Bank Deposits
- Relies upon System of Ledgers
- Very Significant Network Effects:
 - Accepted for Taxes
 - Legal Tender for All Debts Public & Private
 - Accepted throughout Economy / Optimum Currency Area



Image by [epSos.de](#) on Wikimedia. CC BY

Money's Future?



© DK. (Publishing) All rights reserved. This content is excluded from our Creative Commons license. For more information, see <https://ocw.mit.edu/help/faq-fair-use/>

Credit Chip
Galactic Republic



Wupiupi
Hutts on Tatooine



© Hasbro. All rights reserved. This content is excluded from our Creative Commons license. For more information, see <https://ocw.mit.edu/help/faq-fair-use/>

Imperial Credit Coin
The Empire

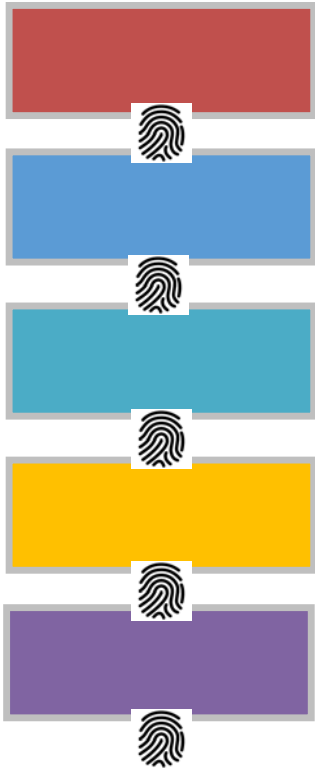
Satoshi Nakamoto: Bitcoin P2P e-cash paper

October 31, 2008

“I've been working on a new electronic cash system that's fully peer-to-peer, with no trusted third party.”

Blockchain Technology

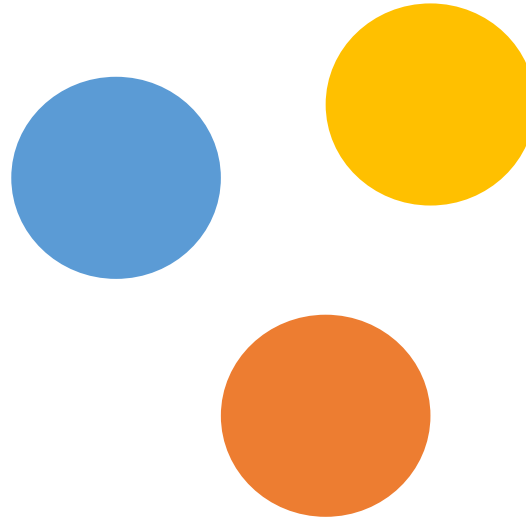
timestamped
append-only ledger



Secured via cryptography

- Hash functions for **integrity**
- Digital signatures for **consent**

multiple party
consensus protocol



Addresses '**cost of trust**'

(Byzantine Generals problem)

May use Native Token as incentive

- Permissioned
- Permissionless

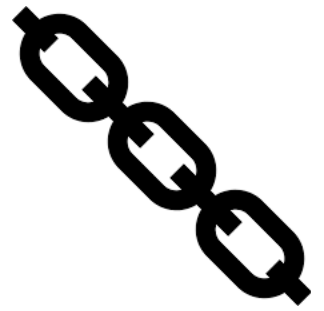
decentralized
auditable database



Tamper resistant record of

- Transfers of **value**
- Running of **computer code**

Smart Contracts



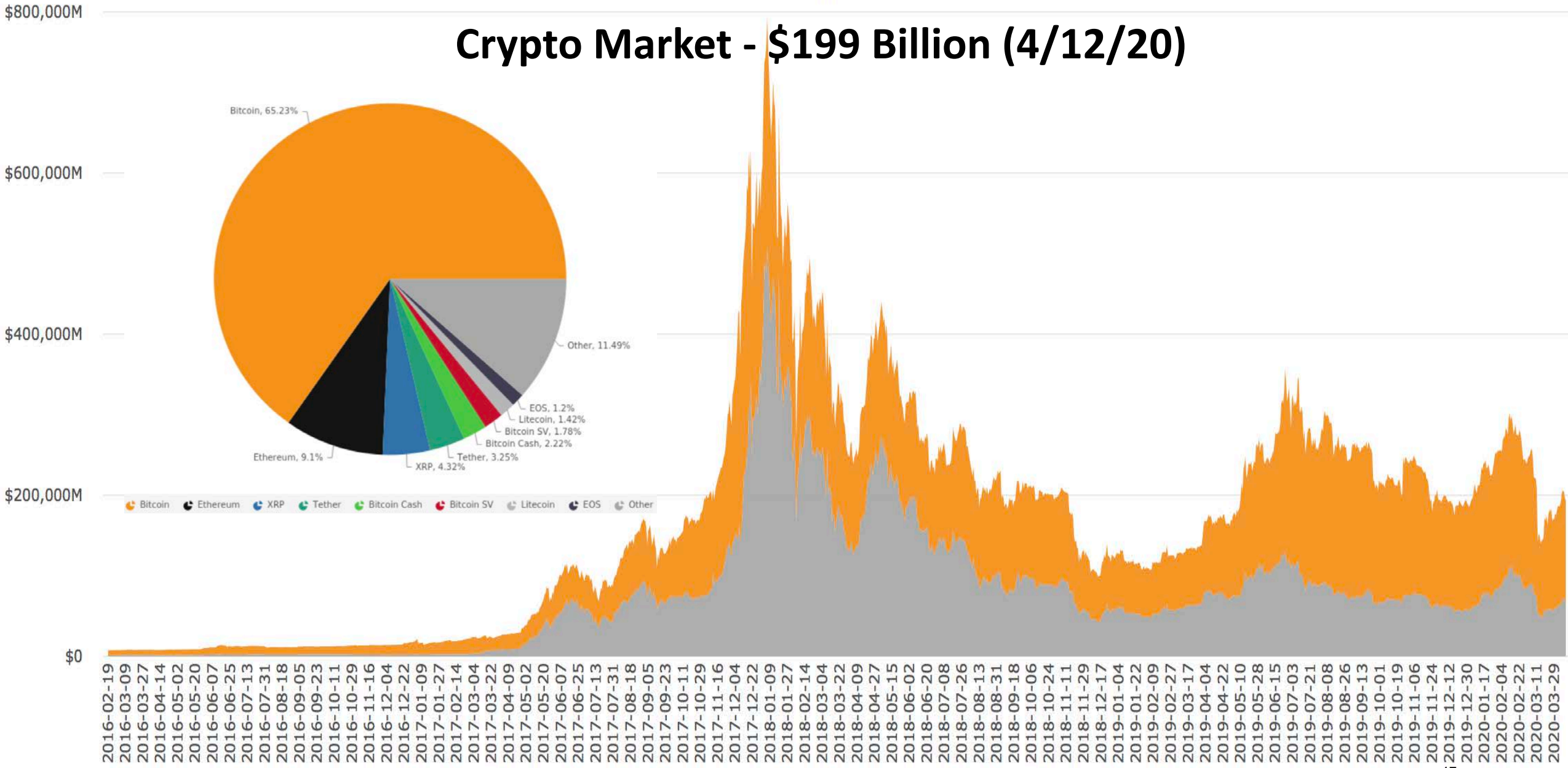
- “A set of promises,
- specified in digital form,
- including protocols
- within which the parties perform on these promises.”

Nick Szabo, 1996

However

- Smart Contracts may not be **‘Smart’**
- Smart Contracts may not be **‘Contracts’**

Crypto Market - \$199 Billion (4/12/20)



Crypto Token Sectors

- **Payment / Store of Value Tokens** \approx **\$152B – 76%**
 - Bitcoin (\$128B), ...
- **Platform Tokens** \approx **\$29B – 15%**
 - Ethereum (\$18B), ...
- **DApp Tokens** \approx **\$10B – 5%**
 - Binance Coin (\$2.3B), ...
- **Stable Value Tokens** \approx **\$8B – 4%**
 - Tether (\$6.4B), ...
- **Tokenized Securities and Assets**

Blockchain Tech Potential Uses

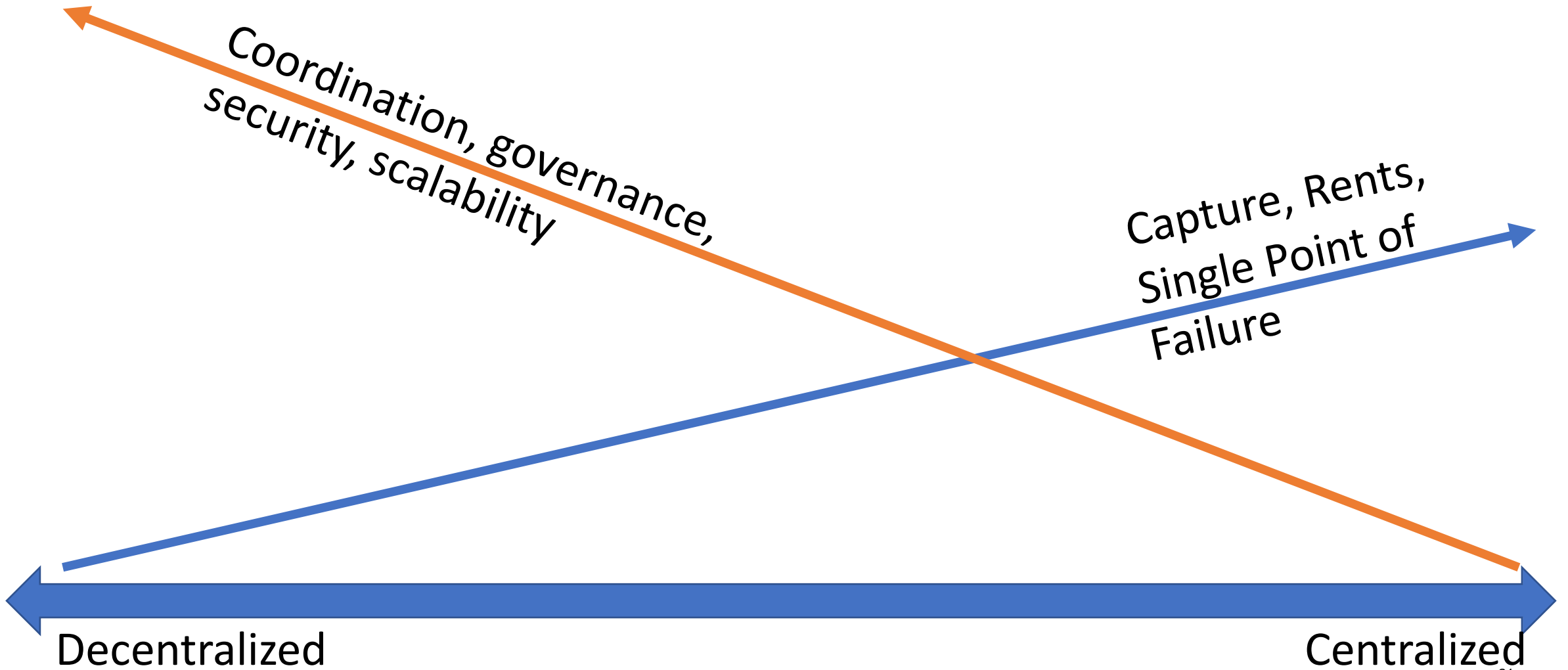
- Speculative Investing
- Crowdfunding through Initial Coin Offerings
- Tokens for Exchanges, Gaming, Gambling, DeFi & File Sharing
- Tokenized Fiat (Stable Value Coins), Securities & Assets
- Payment Systems
- Trade Finance & Supply Chain Management
- Clearing, Settlement & Processing
- Central Bank Initiatives
- Digital ID & MIT Diploma
- Medical Records, Property Records, Internet of Things, Voting ...

Blockchain Technology Challenges

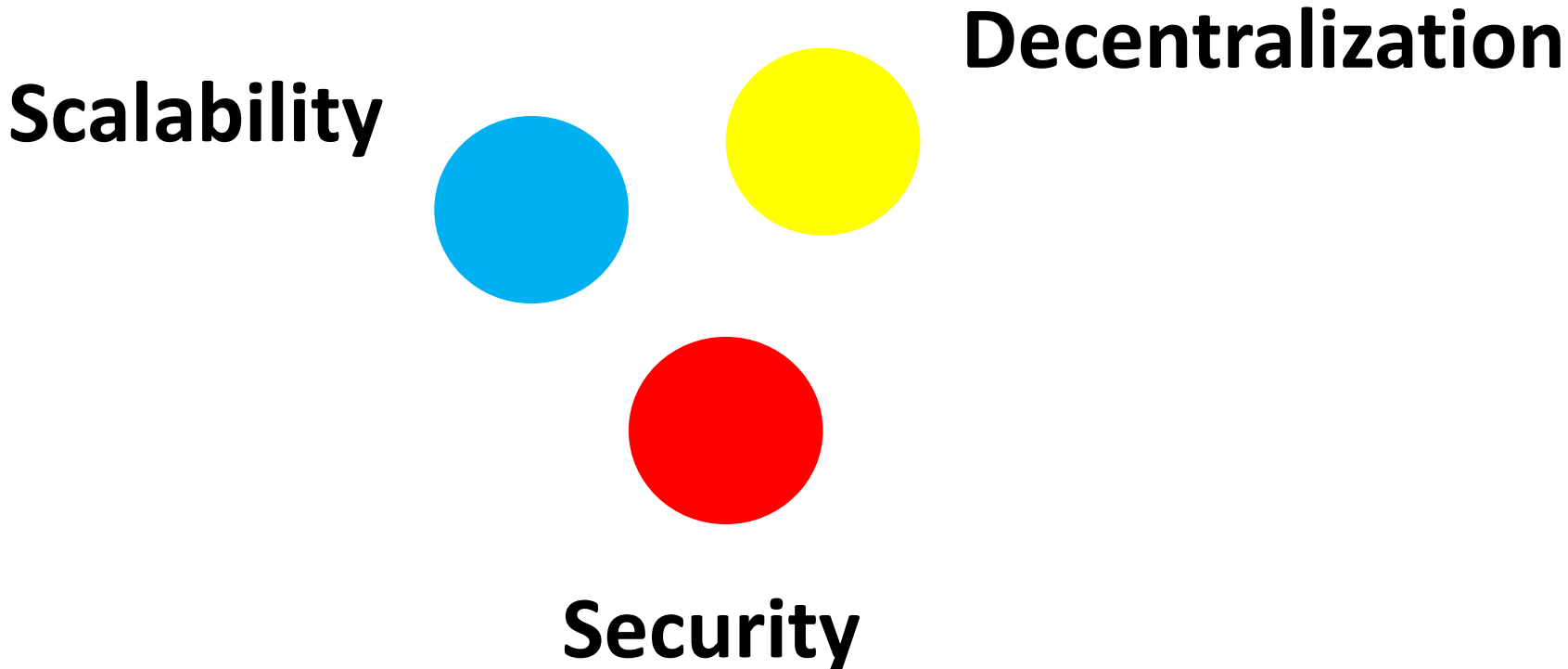
- Scalability, Performance & Efficiency
- Privacy
- Security
- Interoperability
- Governance

- Public Policy Frameworks
- Commercial Use Cases

Framework for Comparing Costs & Trade-offs (Coase)



Vitalik Buterin Trilemma



Assessing Use Cases – First Considerations

Which side of a divide the project is on?

Is the project one that services the new crypto asset class?

Is the project one uses blockchain technology and cryptocurrencies?

Projects servicing the cryptocurrency space:

Custody solution – Coinbase, Fidelity

Software provider – Blockstream

Hardware company – BitMain

Mining pool operator – BTC, F2Pool, Poolin

Exchange operation – Binance, Coinbase

Wallet provider – Circle

Asset manager – Bitcoin Suisse, Galaxy

News service – CoinDesk

Assessing Use Cases – Strategic Considerations

- What value creation proposition is there?
 - Decentralized vs. Centralized Computing?
 - Native Token filling what Gaps in Fiat Currency system?
- What are competitors (Traditional & Blockchain) doing?
- Why use append only ledgers, multiple party consensus and native token?
- What verification or networking costs can actually be reduced?

Assessing Use Cases – Tactical Considerations

- Which data needs recording on append-only ledgers?
- Which multiple stakeholders need ‘write’ access to the shared ledger?
- What are the tradeoffs of performance, privacy, security, governance & regulation?
- How can broad adoption and user interface be realized?
- If permissionless, what are the token incentive systems?

Assessing Use Cases – Deeper dive

- Why use multiple party shared ledger?
 - Why choose a distributed ledger solution over a centralized one?
 - Why not rely on a third-party authority or host?
 - Is the value proposition well distributed amongst all parties?
 - What is the adoption model?
- What specific verification or networking costs can be reduced?
 - Authentication? Traceability? Trust?
 - Are the transaction processes & data standardized?
 - How much data needs to be stored?

Incumbents' Choices of Databases

Access



Client Server

Permissioned

Permissionless

Traditional Databases

Trusted Party Hosts Data

Trusted Party can Create, Read, Update, & Delete (CRUD)

Client Server Architecture

Private Blockchain

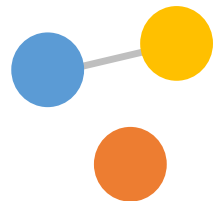
Known Participants

Private Write Capability

Append Only Timestamped Log

Publicly Verifiable

No Native Currency Needed



Public Blockchain

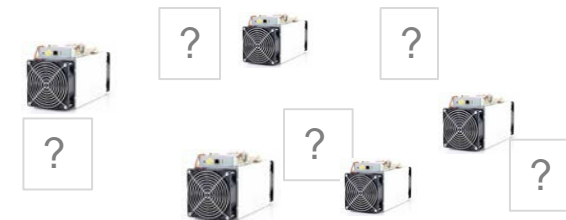
Unknown Participants

No Central Intermediaries

Public Write Capability

Peer to Peer Transactions

Native Tokens & Incentives



Central Bank Initiatives

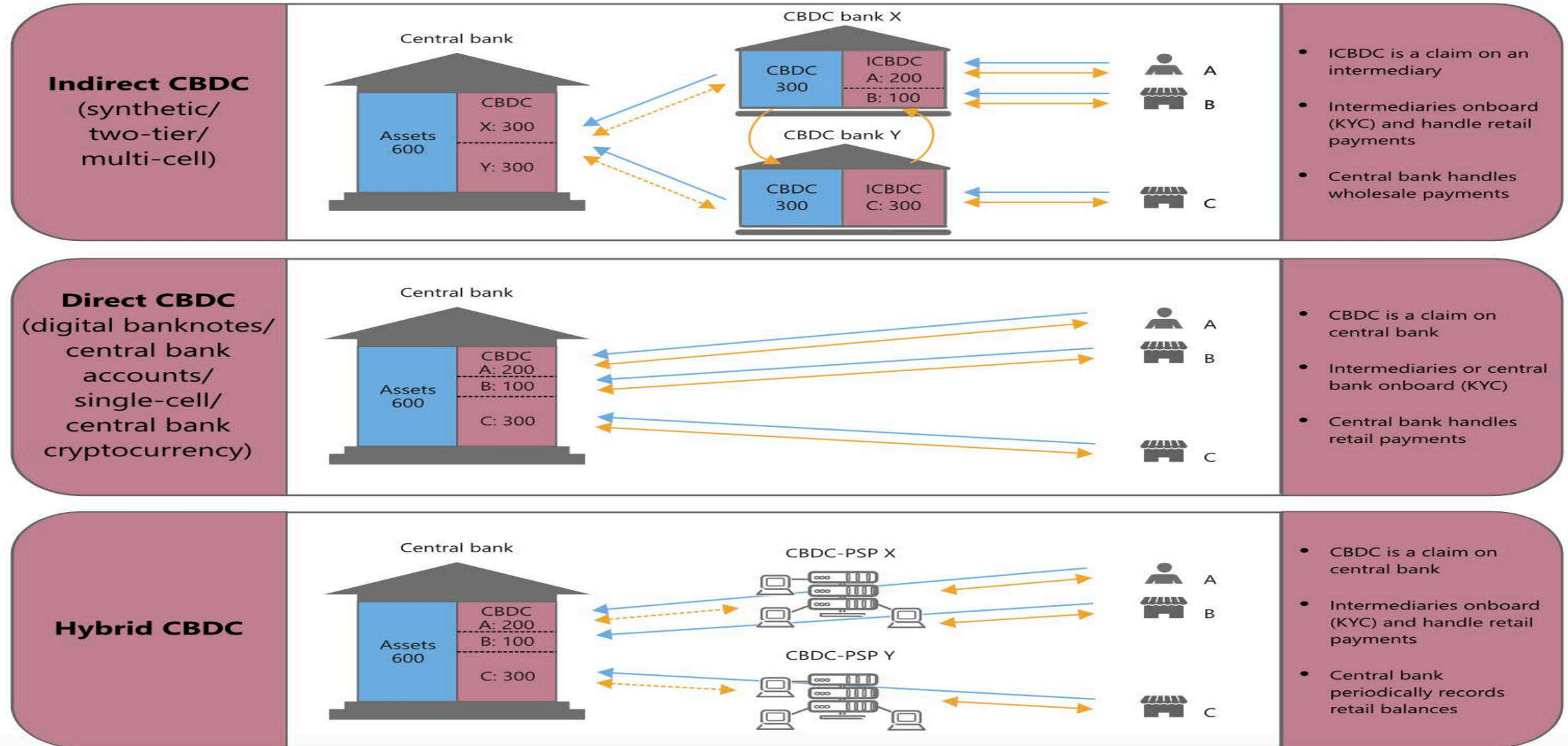
Real Time Gross Settlement

- Brazil, Canada (Project Jasper), Europe and Japan (Project Stella), Singapore (Project Ubin), South Africa (Project Khokha)

Digital Currency

- Central Bank Claim: Bahamas (Sand Dollar), Ecuador (Dinero Electrónico), Iran (Payman), Sweden (E-Krona)
- Commercial Bank Claim: Philippines (ePiso), Senegal (eCFA), Tunisia (e-Dinar)
- Possible Hybrid: China (Digital Currency Electronic Payment)
- Commodity Backed: U.K. (Royal Mint Gold), Venezuela (Petro)
- Other: Dubai – emCash, Saudi & UAE (cross-border pilot), Uruguay (Digital Peso)

CBDC Potential Architectures



CBDC – Opportunities

- Continue Government Provision of a Means of Payment
- Promote Competition in Banking System
- Promote Financial Inclusion & P2P Payments
- Address Payment System ‘Pain Points’
- For Some Nations, Possibly Avert Sanctions

CBDC - Challenges & Uncertainties

- Financial Stability and Potential to Increase Ease of Bank Runs
- Changes to Commercial Banks' Deposits and Funding Models
- Effects on Credit Allocation and Economy
- Monetary Policy Implementation & Transmission
- Resilience of Open Payment Infrastructures

Ground Truths

- Nakamoto solved the payments riddle - avoiding double spending
- Money is but a social & economic construct
- We already live in an age of digital money
- Append-only logs & multiparty consensus provides a peer-2-peer alternative
- Blockchain technology can address verification and networking costs
- Adoption rests on addressing comparative viability & value proposition

Ground Truths

- Crypto markets are rife with scams, fraud, hacks & manipulation
- Cryptocurrencies have evolved into a speculative asset class
- Crowdfunding built on smart contracts & ICOs raised nearly \$30 billion
- Lightly & non regulated markets provide retail investors direct way to trade
- The potential, though, to be a catalyst for change is real

MIT OpenCourseWare
<https://ocw.mit.edu/>

15.S08 FinTech: Shaping the Financial World
Spring 2020

For information about citing these materials or our Terms of Use, visit: <https://ocw.mit.edu/terms>.